PREVENTION OF NODE CLONE ATTACK: SECURE AND ENERGY EFFICIENT ALGORITHMS IN WSN

Synopsis submitted in fulfillment of the requirements for the Degree of

DOCTOR OF PHILOSOPHY

By

VANDANA MOHINDRU

Enrolment No. 136210

Under the Supervision of

Dr. Yashwant Singh and Dr. Ravindara Bhatt

Department of Computer Science Engineering and Information Technology

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY

Waknaghat, Solan-173234, Himachal Pradesh, INDIA

22nd November, 2018

Table of Contents

Table of Contents Page Numbers

ABSTRACT

CHAPTER-1

INTRODUCTION **5**

1.1 Introduction **5**
1.2 Genesis of Problem **5**
1.3 Problem Statement **5**
1.4 Objectives **6**
1.5 Approach Followed **6**
1.6 Contributions **6**
1.7 The Organization of Thesis **7**

CHAPTER-2 **8**

REVIEW OF LITERATURE **8**
2.1 Introduction **8**
2.2 Security in WSNs **8**
2.3 Security Attacks In WSNs **8**
2.4 Node Clone Attack **9**
2.5 Analysis of Node Clone Detection Methods **10**

CHAPTER-3

SECURING WIRELESS SENSOR NETWORKS: NODE CLONE ATTACK **13**
3.1 Introduction **13**
3.2 Proposed Algorithm **13**
3.3 Analysis of Proposed Algorithm **14**

CHAPTER-4

NODE AUTHENTICATION: NODE CLONE ATTACK **16**
4.1 Introduction **16**
4.2 Algorithm Assumptions **16**
4.3 Proposed Node Authentication Algorithm **16**
4.4 Performance Analysis of Proposed Node Authentication Algorithm **18**

CHAPTER-5

MESSAGE AUTHENTICATION: NODE CLONE ATTACK **21**
5.1 Introduction **21**
5.2 Proposed Message Authentication **21**
5.3 Results and Analysis of Proposed Message Authentication Algorithm **22**

CHAPTER-6

MOBILE NODE AUTHENTICATION IN WIRELESS SENSOR NETWORKS **25**
6.1 Introduction **25**
6.2 The Proposed Protocol for Mobile Node Re-Authentication **25**
6.3 Performance Analysis **27**

CHAPTER-7

CONCLUSION AND FUTURE SCOPE OF WORK **29**

7.1 Introduction **30**

7.2 Limitations of Work **30**

7.3 Future Work **30**

REFERENCES **31**

PUBLISHED PAPERS **34**

ABSTRACT

Nowadays, Wireless Sensor Networks (WSNs) are becoming one of the best choices for monitoring and surveillance application. WSNs are a promising candidate in applications such as healthcare, agriculture, military etc. The reason for the growing popularity of sensor networks is the lightweight sensor nodes. These small sized cost-effective nodes are battery constrained devices with limited computation power and work within short ranged using wireless communication. These sensor nodes are spatially dispersed in the hostile environment where there is no involvement of human being. The primary motive of these sensor nodes is to sense the physical occurrences in the region-of-interest and perform processing after that transfers the sensed data to the base station. In WSNs, multi-hop communication is preferred for a scalable network. Further, sensor nodes are resource constraints in terms of power, computation energy, communication energy, and storage space. The sensor nodes in WSNs are easily approachable by various attackers because sensor nodes are unattended in the hostile environment. An attacker can easily capture sensor nodes, altering information being communicated and reducing the capability of the sensor networks to carry out its tasks. There are frequent security attacks in the network. Some of them are node clone attack, Sybil attack, sinkhole attack, traffic analysis attack, wormhole attack, replay attack, black hole attack, and Denial of Service (DDoS) attack. All these attacks have different goals and consequences. Further, these attacks work at different levels during the network lifetime. Out of these security attacks, node clone attack is one of the most dangerous attacks. In this thesis, we consider node clone attack and proposed the algorithms that secure sensor networks from the node clone attack. In node clone attack, the attacker compromises the sensor node which is placed in an unattended environment and extracts sensor node secret information like keys and node identification details.

Soon after, the attacker starts to replicate the vast number of clones of compromised node throughout the sensor network. These clone nodes behave like legitimate nodes and slowly start getting the attention which will results in the participation of clone nodes in network functioning. This node clone attack further results in several internal as well as external attacks in WSNs.

Therefore, security in WSNs becomes one of the significant issues that have taken the attention of many researchers. In spite of the extensive research, the security standard which secures energy-constrained wireless sensor networks from various critical attacks is required for WSNs. Thus, it is necessary to balance the deployment of WSNs which involves cautious decisions and trade-offs between energy consumption and security. To provide a security countermeasure for every possible attack would result in an enormous amount of overheads in WSNs. So there is a need to design lightweight security algorithms that consume less energy, memory and processing competences of sensor network nodes.

This thesis work is carried out to secure sensor nodes as well as message communication in WSNs from node clone attack. Firstly, hybrid cryptography algorithm is proposed which secure message communication in WSNs. The hybrid cryptography algorithm uses a combination of AES and ECC cryptography for maintaining the integrity of messages. A

number of evaluation metrics are used for assessing the performance of the proposed hybrid algorithm. This algorithm does not provide the optimal solution for energy constrained sensor networks. Therefore, an energy efficient node authentication algorithm is proposed which is used for securing and authenticating sensor nodes in WSNs. This proposed algorithm checks the originality of each sensor node in WSNs and easily detects cloned nodes. To check the authenticity of messages during message communication, a novel message authentication algorithm is proposed. This algorithm secures messages that can be interpreted during network communication by attackers. The proposed message authentication algorithm is lightweight nature and maintains the integrity of messages. Wireless sensor networks consist of both stationary sensor nodes as well as mobile sensor nodes. The above discussed proposed algorithm secures stationary sensor nodes only therefore, another algorithm is proposed that secure mobile nodes in WSNs. For securing mobile sensor nodes an energy-efficient, the low overhead re-authentication scheme is proposed. The position of mobile nodes is dynamic as mobile nodes move from one region to another region based on their interest. This re-authentication scheme provides security to the mobile nodes in WSNs.

The proposed work in the thesis secures sensor nodes (static and mobile) and message communication inside the sensor networks. Further, the proposed work may be exploited on different applications of WSNs.

CHAPTER 1
INTRODUCTION

1.1 Introduction

Wireless Sensor Networks (WSNs) are becoming popular nowadays. WSNs are widely used in monitoring and surveillance applications due to low-cost of sensor nodes, unattended nature of deployment and the capability of self-organization of sensor nodes [1]. Security is vital for many sensor network applications, such as military target tracking, weather monitoring, forest fire detection, and habitat monitoring [2], [3]. Securing communication in these types of networks not only desires to provide the fundamental security but also needs confrontation against countless external attacks. Message authentication and message integrity is a severe concern for sensor networks security; therefore, WSNs must guarantee the distribution of genuine message without any modification or amendment of the message [4]. Mobile Wireless Sensor Networks (MWSNs) consists of a fraction of mobile nodes along with static nodes [5]. Further, the security of these mobile nodes is an important issue due to the dynamic nature of the mobile nodes.

1.2 Genesis of Problem

The wireless sensor network is prone to various types of security attacks, but this thesis focuses on node clone attack. The node clone attack is the most critical attack because it becomes a source of other attacks like Wormhole Attack, Sybil Attack, and Denial of Service Attack. The foremost challenge is to provide an energy-efficient security solution feasible to implement in a resource-constrained environment in WSNs. Authentication is the one of the most critical security requirement for energy constrained WSNs. The Authentication can be achieved in terms of node authentication, message authentication and mobile node re-authentication. In order to secure Wireless Sensor Networks the following research issues are as follows: lack of energy efficiency mechanism, lack of sensor node security, insecure message communication and lack of mobile node authentication

1.3 Problem Statement

Wireless sensor networks are vulnerable to node clone attack. Thus there is a need for a security mechanism against the node clone security attacks. Further, the security solution against the node clone attack should be energy-efficient for the resource-constrained environment in wireless sensor networks. The security mechanism should be light-weight and should require limited storage overheads, a small number of computation steps, and a small number of message communications among sensor nodes. The authentication of sensor nodes in the initial stages is an important step in WSN. Thus the process of finding the node clones in the initial stage helps in an effective security of WSN. The mobile nodes are advantageous for the quality of service parameters in WSN. Thus re-authentication is an important step in mobile wireless sensor networks.

1.4 Objectives

The following objective has been articulated, on the basis of the above problem statement and accomplished in this research work.

a) To develop a new hybrid cryptography algorithm for securing wireless sensor networks from node clone attack.

b) To develop an energy efficient node authentication algorithm for WSNs for securing static sensor nodes in wireless sensor networks from Node Clone Attack.

c) To develop a message authentication algorithm for securing message communication within wireless sensor networks from node clone attack.

d) To develop a mobile node authentication algorithm for wireless sensor networks for securing mobile wireless sensor nodes from the various security attacks.

1.5 Approach Followed

Securing wireless sensor networks from the node clone attack is one of the most difficult tasks. Moreover, detection of clone nodes is an important step in wireless sensor networks. For securing WSN from node clone attack, a hybrid cryptography algorithm is proposed. This algorithm uses properties of AES (Advanced Encryption Standard) [6] and ECC (Elliptic Curve Cryptography) cryptography algorithms [7] and provides enhanced security to the wireless sensor networks. The proposed algorithm is then compared with the other algorithms present in the literature. A number of evaluation metrics are used to check the performance of the proposed algorithm. An energy efficient authentication mechanism is designed to secure sensor nodes from the attacker. The proposed mechanism authenticates each sensor node before communication takes place within WSNs. This node authentication mechanism works on the sender and receiver sides. At sender node side different methods like key formulation, encryptions, embedding of keys are applied in order to compute 24-bit encrypted unique identity. To overcome the problem of message modification during communication, a lightweight message authentication algorithm is devised. In this message authentication algorithm, a light weight hash function is used which convert the arbitrary length of the message to fixed size hash digest. Finally, to solve the problem of mobile node authentication, a re-authentication scheme is proposed which secure the mobile nodes in WSNs. The proposed re-authentication scheme utilizes mobile node management, network setup phase, the registration phase of the mobile node, mobile re-authentication phase, on-demand route setup phase.

1.6 Contributions

In this thesis we explore various factors affecting the security in WSNs. In chapter 2, we surveyed the existing security attacks in WSNs and present a comparison between various security attacks. Further, this thesis focuses on one of the most dangerous attack i.e. Node Clone Attack. The proposed algorithm in chapter 3 uses the hybrid cryptography techniques that consist of AES, ECC and lightweight hash function. The hybrid cryptography algorithm consumes an ample amount of the sensor node energy and makes WSNs unproductive. Therefore, Chapter 4 introduces a new energy efficient node authentication algorithm. The proposed node authentication algorithm, authenticate each node before network operation starts. After authenticating sensor nodes next step is to authenticate message during communication within the sensor network. Therefore, chapter 5 presents the novel message authentication algorithm which secures messages from being modified during the time of

network operation. The proposed node authentication and message authentication algorithms work efficiently for static sensor nodes. Chapter 6 presents the mobile node authentication in wireless sensor networks. This proposed algorithm uses re-authentication because re-authentication is important for a mobile node as the node moves from one region to another region in the RoI (Region of interest).

1.7 The Organization of the Thesis

Chapter 1 provides the basic introduction of wireless sensor networks, problem statement and objectives. **Chapter 2** discusses a detailed literature survey on WSN, security issue, attacks and focus on node clone attack. **Chapter 3** presents the newly proposed hybrid cryptography algorithm for securing WSNs from node clone attack. Node authentication algorithm which is designed for securing static sensor nodes from the effect of node clone attack in WSNs is presented in **Chapter 4.** Further, **Chapter 5** presents a novel lightweight message authentication algorithm that secures message communication within WSNs. **Chapter 6** provides a solution for securing mobile sensor nodes in WSNs. This chapter discusses a new Mobile node authentication in WSNs. Finally, **Chapter 7** concludes the thesis with a brief discussion on the possible extension to our work in the future. This chapter also describes direction for the future work.

CHAPTER 2
REVIEW OF LITERATURE

2.1 Introduction

WSNs consist of plentiful sensor nodes with processing, sensing, communication, and storage competences [8]. All these sensor nodes are disseminated in an intimidating environment to observe and react to changes in the physical phenomena of their surroundings (Figure 2.1).

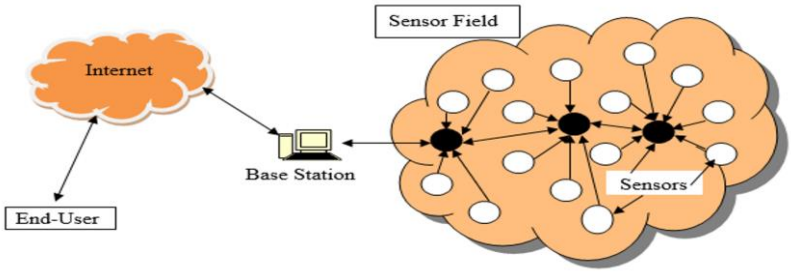


Figure 2.1 WSN

2.2 Security in WSNs

WSNs are widely used these days due to the wide areas of applications such as military, health, environmental, commercial and agriculture, therefore need for effective security mechanisms is very important [9], [2]. Security in these WSNs is a most challenging task because:

- WSNs can be deployed in large scale for safety-critical applications.
- Open-shared communication medium.
- Distributed Network architecture
- Lack of Physical Protection.
- Transmissions are highly vulnerable to malicious internal and external attackers.
- Security is crucial for ensuring smooth network operations.
- Node deploys in hostile environments.
- Unattended nature of WSNs.
- Sensor node constraints make WSNs more vulnerable to DoS attack.
- An adversary can spoof out the subtle information and can interrupt the network processes.

2.3 Security Attacks in WSNs

WSNs are susceptible to numerous security attacks. Security attacks are classified on the basis of damage/ access level, attacker's position, attacking device, information in transit and protocol stack. A brief enumeration of attacks is presented as in figure 2.2.

2.4 Node Clone Attack

In WSNs, nodes are arranged in the unfriendly environments where nodes can be physically caught and compromised by an adversary. After compromising sensor node, adversary extracts confidential information (keys) from the genuine node and inserts clones of a

compromised node within the wireless sensor network. This is called Node clone attack as shown in Figure 2.3.

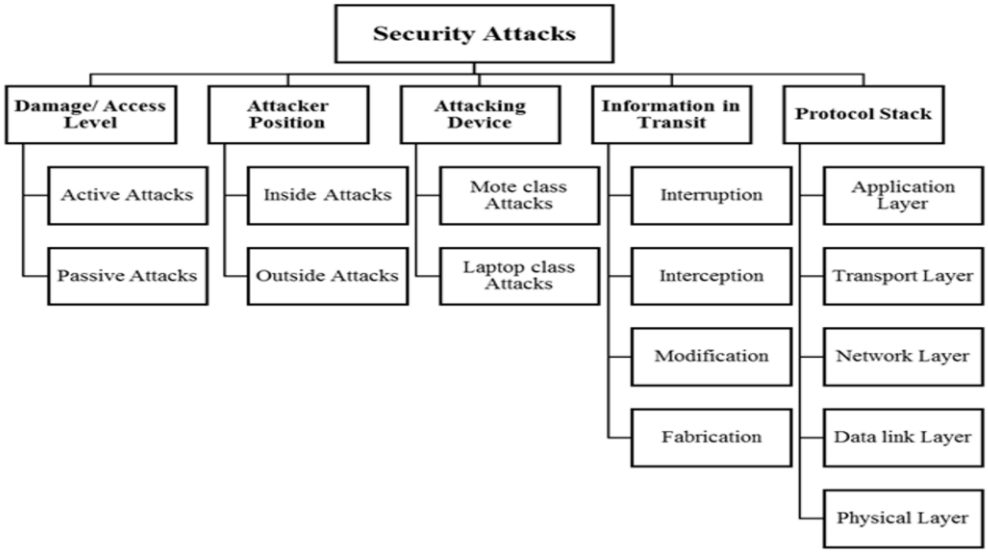


Figure 2.2. Classification of Security Attacks in WSNs

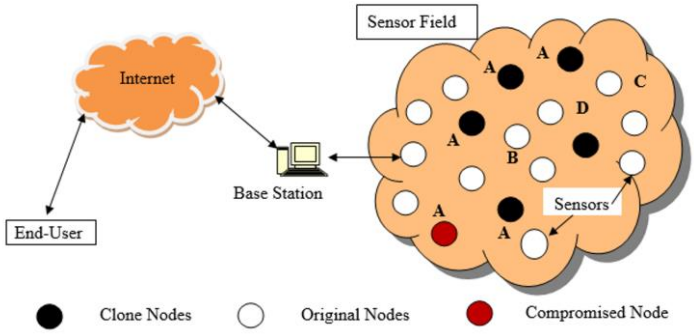


Figure 2.3. Node Clone Attack Example

2.4.1 Node clone attack detection methods

Node clone detection methods are classified into two types: Centralized and distributed detection methods [10], [11], [12]. In the centralized detection method, base station acts as the central entity which is responsible for all decision making and in distributed detection method no such central entity exists. Every sensor node takes part in decision making. The main goals of detection methods are:

- The detection methods must have minimum communication cost, low memory consumption, less energy use, computational overhead, maximum detection probability and security level.
- The detection methods must be strong enough against attacker's effort to break them.
- The detection methods must detect and revoke only compromised and clones or replica nodes of the sensor networks.

2.5 Analysis of Node Clone Detection Methods

Table 2.1. Classification and Comparison of Node Clone Detection Methods in WSN

Methods	Sensor Type	Approach Used	Deployment	Area Detection	Communication cost	Memory Cost	Detection level
Base Station (BS) based	Static	Centralized	Random Uniform	Whole area detection	O (n √n)	O(d)	High, if all messages reach the base station.
SET	Static	Centralized	Random Uniform	Whole area detection	O (n)	O (d)	High
Random key predistribution	Static	Centralized	Random Uniform	Whole area detection	O (n log n)	O (d)	High
Real time clone detection using fingerprints	Static	Centralized	Random Uniform	Whole area detection	O (num_m√n). log2M	O(d) + min(M ,ω . log2 M)	High
Hierarchical Node Replication Detection	Static	Centralized	Random Uniform	Whole area detection	O(t2)	O(t)	High
Compressed Sensing-Based Clone Identification(CSI)	Static	Centralized	Random Uniform	Whole area detection	$O(n \log n)$	O(n)	High
Fast and effective mobile replica node detection	Mobile	Centralized	Random Uniform	Whole area detection	O(n √n)	O(n)	High
New Protocol for the Detection of Node Replication	Mobile	Centralized	Random Uniform	Whole area detection	$O(n \log n)$	O(n)	High
Node-To-Network Broadcasting	Static	Distributed	Random Uniform	Whole area detection	$O(n^2)$	O (d)	High, if the broadcasts reach every node.
Deterministic Multicast	Static	Distributed	Random Uniform	Whole area detection	O(g ln g √ n / d)	O (g)	Low

Methods	Sensor Type	Approach Used	Deployment	Area Detection	Communication cost	Memory Cost	Detection level
Randomized multicast	Static	Distributed	Random Uniform	Whole area detection	O (n^2)	O (√n)	Medium
Line selected multicast (LSM)	Static	Distributed	Random Uniform	Whole area detection	O (n √n)	O (√n)	Medium
Randomized, Efficient, and Distributed (RED)	Static	Distributed	Random Uniform	Whole area detection	O (√n)	O (d √n)	High
Active detection	Static	Distributed	Random Uniform	Whole area detection	O (√n)	O(1)	Low
Random-Walk Based detection	Static	Distributed	Random Uniform	Whole area detection	**RAWL:** O(√n log n) **TRAWL:** O(√n log n)	**RAWL:** O(√n log n) **TRAWL:** $O(1)^2$	High
Localized Multicast	Static	Distributed	Grid	Whole area detection	O (√n)	O (√n)	High
Distributed hash table (DHT)	Static	Distributed	Random Uniform	Whole area detection	O (log n √n)	O (d)	High
Randomly directed exploration	Static	Distributed	Random Uniform	Whole area detection	O (√n)	O (d)	Medium
Group-based clone detection	Static	Distributed	Grid	Local area Detection	**BASIC:** O(m) **LCA:** O(m+d) **MGA:** 3O(m+d)	**BASIC:** O(m) **LCA:** O(d+2m) **MGA:** O(d+2m(1+D_{max}))	**BASIC:** Low **LCA:** High **MGA:** High

Methods	Sensor Type	Approach Used	Deployment	Area Detection	Communication cost	Memory Cost	Detection level
Random Walk with Network Division (RAND)	Static	Distributed	Random Uniform	Whole area detection	O(log n)	O(log n)	Higher than RAWL
Random Walk with Network Division (RWND)	Static	Distributed	Random Uniform	Whole area detection	O(log n)	O(log n)	Higher than RAND
Single Stage Memory Random Walk with Network Division (SSRWND)	Static	Distributed	Random Uniform	Whole area detection	O(log n)	O(log n)	Higher than SSRWND
Extremely Efficient Detection (XED)	Mobile	Distributed	Random Uniform	Whole area detection	O(1)	No Storage required	Medium
Efficient and Distributed Detection of Node Replication Attack	Mobile	Distributed	Random Uniform	Whole area detection	EDD: O(1) SEDD: O(n)	EDD: O(n) SEDD: $O(\xi)$	High
Patrol-based Replica Detection	Mobile	Distributed	Random Uniform	Local area Detection	O(n* $\sqrt{k}$)	O(n)	High
Single-Hop Detection (SHD)	Mobile	Distributed	Random Uniform	Whole area detection	O(n)	O(n)	High
Mobility-Assisted Detection	Mobile	Distributed	Random Uniform	Whole area detection	UTLSE: $O(n)$ MTLSD: $O(n)$	UTLSE: $O(\sqrt{n})$ MTLSD: $O(\sqrt{n})$	Medium

From the comparative analysis table and above theoretical discussion, it can be analyzed that distributed detection methods are preferred over centralized detection methods because of the single point failure problem with centralized detection methods. All the methods use the different assumptions and thus have their respective strengths and weaknesses, so it is difficult to make out which one is better over another. Hence, a lot more work is needed to do with making detection methods energy efficient so that the quality and performance of WSNs will preserve.

CHAPTER 3
SECURING WIRELESS SENSOR NETWORKS: NODE CLONE ATTACK

3.1 Introduction

In this chapter we present a hybrid cryptography technique which provides the solution towards the above-said problem. This hybrid technique provides a high level of security in WSNs and also shields it from the consequence of critical node clone attack. Also, this technique secures message communication in wireless sensor networks.

3.2 Proposed Algorithm

The proposed algorithm comprises of: AES, ECC and lightweight hash function algorithm. The algorithm consists of two components. The first component runs on a sender node. The second component runs on the receiver node. We assume A as the sender node and B as the receiver node.

Sender Node:

Algorithm S

Input: Message of arbitrary length.

Output: Cipher text for receiver node B.

1. We assume that node A wants to communicate with node B. Firstly, arbitrary length message of node A initially move to lightweight hash function module so that hash digest H is generated as presented in figure 3.2.
2. A pseudo-random generator is used so that Session key (K_s) is calculated.
3. Now H hash digest goes to ECC encryption module to calculate digital signature by applying private key of sender node. Also, private key K_{AES} is encrypted by the ECC module.
4. Digital signature and plain text message are further going to AES encryption module and result in the cipher text signature.
5. At last, the complete cipher text is communicated to sensor node B.

Receiver Node:

Algorithm R

Input: Cipher text received by the sender node.

Output: Message authentication successful or unsuccessful.

1. Receiver node B has cipher text received from node A. By using own private key node B decrypt the AES key i.e. K_{AES} using ECC decryption module as presented in figure 3.3.
2. Now, AES decryption module decrypts cipher text and signature cipher by using K_{AES}.
3. ECC decryption module uses node A public key for verification of the signature & generate H'.
4. Plaintext moves to lightweight hash function module and results in H hash digest.
5. In the last step, both calculated H with H' are compared with each other. If both H and H' match with each other than the message is authenticated else message is altered by the cloned node.

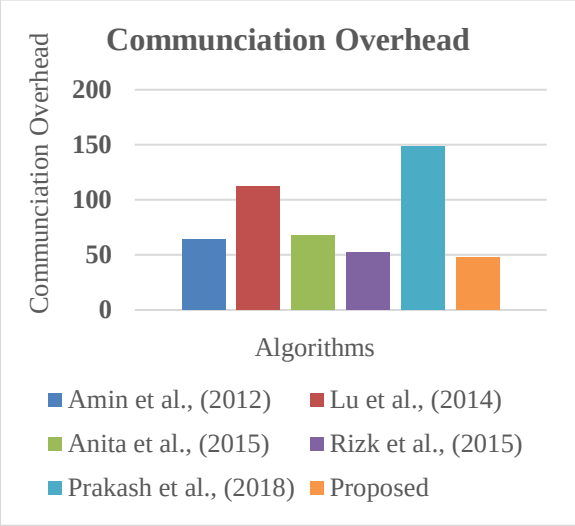
The above proposed algorithm designed to secure message communication in WSNs. In the algorithm, H (sender calculated hash digest) and H' (receiver calculated hash digest) are compared with each other to check the originality of the message being communicated. If the H and H' match with each other than the message is regarded as authentic and if does not

match the sender node consider to be clone node and an alert message is broadcasted in the WSNs. The base station further discards the cloned node from the sensor network. By doing these WSNs maintains its security.

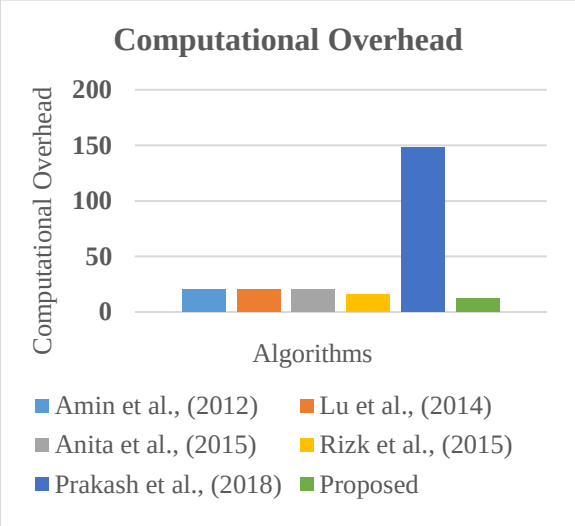
3.3 Analysis of Proposed Algorithm

Various metrics are mentioned below that are used to compute the performance of the proposed algorithm:

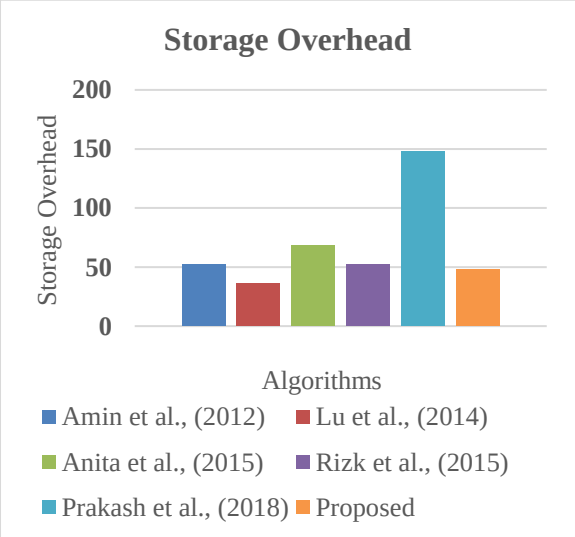
a) Communication overhead: For wireless sensor networks, communication overhead is computed by the energy disbursed while transmitting one byte of data from one sensor node to another. From the figure 3.1 (a), it can be analyzed that Lu et al., [30] has very high communication overhead as related to other algorithms present in the literature. The proposed consider being efficient in terms of communication overhead as it consumes less sensor node energy while message transmitting. Rizk et al., [29] also have lower communication overhead on the other side Prakash et al., [37] have higher communication overheads.



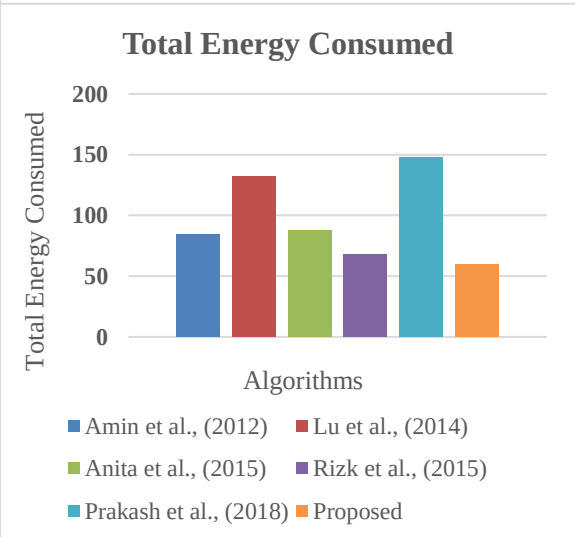
(a)



(b)



(c)



(d)

Figure 3.1 a) Communication Overhead b) Computation Overhead c) Storage Overhead d) Total Energy Consumed

b) Computational overhead: Computational overhead for WSNs can be defined as the amount of energy dissipated during algorithm execution. For proposed algorithm, communication overhead is computed as the quantity of energy dissipated through encryption, decryption and hash function processing. The algorithms Amin et al., [28], Lu et al., [30] and Anita et al., [31] have almost similar computational overhead but Prakash et al., [37] have higher computational overhead. The proposed algorithm has lower computational overhead as related to the other hybrid cryptographic algorithms as depicted infigure 3.1 (b).

c) Storage overhead: Nodes in WSNs are small in size due to which they have a limited amount of memory or storage space for storing information. In WSNs, storage overhead is computed as the volume of information stored in the memory of sensor nodes. The proposed algorithm uses AES and ECC cryptography algorithms, energy efficient hash function for securing message communication. These algorithms require less space in sensor node memory because encryption key size is small and hash function has fixed 96-bits size. From the figure 3.1 (c), it can be analyzed that the Lu et al., [30] has minimum storage overhead as compared to all algorithms and our proposed algorithm stands second in terms of lower storage overhead.

d) Total energy consumed: In wireless sensor networks, total energy disbursed by each sensor node can be computed as the sum of energy dissipated through communication and computation tasks of algorithm. Therefore, in the proposed algorithm minimum sensor node energy consumed during communication and computation tasks as related to other algorithms as shown in figure 3.1 (d). Also, Rizk et al., [29] have minimum total energy consumed and Lu et al., [30] and Prakash et al., [37] has higher total energy consumed among all algorithms.

e) Security level: The key prerequisite of any WSNs algorithm is higher security level by attaining certain security goals like confidentiality, integrity and authentication. All the algorithms discussed in the literature provide security in the WSNs by accomplishing different security goals. The proposed algorithm offers a higher level of security by using AES cryptographic algorithm for encryption and a hash function for calculated fixed size small 96-bit hash digest. Further, the ECC algorithm in our work enhances the security by encryption of the secret key.

Therefore, from the above discussion, it can be analyzed that the proposed algorithm has lower computational and communication overheads but add little more of storage overhead in WSNs. The proposed algorithm uses AES, ECC as cryptographic algorithms and lightweight hash function which maintain authentication as well as the integrity of the message in WSNs. Also, the proposed algorithm is perfectly suited to the various WSNs applications.

CHAPTER 4
NODE AUTHENTICATION: NODE CLONE ATTACK

4.1 Introduction

Wireless Sensor Networks (WSNs) consists of energy-constrained sensors nodes. These energy-constrained nodes are positioned in the Region-of-Interest (RoI) with the help of a mathematical model. Attacker generates obstacle in the normal working of WSNs as these networks are left unattended in vulnerable environment. Various node clone attack detection methods present in the literature and these methods provide security to the network but on the same side violate the other parameters like communication cost, computation cost and storage cost of sensor nodes. Therefore, in this chapter we present a novel node authentication algorithm which checks the authenticity of the sensor nodes earlier than communication starts. To check the authenticity of nodes before message communication is important because clone nodes are recognizing at the very initial step of network functioning.

4.2 Algorithm Assumptions

We expect that every sensor node has their unique 32-bit ID and pre-defined location. Likewise, every node knows similar data, i.e. ID and location of the 1-hop neighboring node. The neighbor list comprises of the 1-hop neighbor node, UIDs of individual neighbor, Location coordinates of individual neighbor.

For Example:

Node B 32-bit UID = 10101111010111001110010100110000

Nodes B Neighbor's = A, C, D, G, H

Location = (X_B, Y_B)

4.3 Proposed Algorithm

The proposed node authentication algorithm consists of two algorithms one is the sender node and another is the receiver node.

Sender Side Algorithm –The sender side involves following three algorithms: Keys Formation, Encryption of Sender Node UID and Keys Embedding.

1. Keys Formation:

Algorithm S1: -
Input: Sender node UID = 32-bit
Output: Two 16-bit keys K1 and K2.
1. Set key K1 = NULL; K2 = NULL;
2. Calculate Random numbers R1 and R2;
3. Set N1 = R1;
4. for (i=2; i<=4; i++)
{
Ni = Ni-1 - 0100;
}
5. Extract four 4-bit numbers from MSB position of UID i.e. T1 to T4
6. N5 = N1 ⊕ T1;

7. N6 = N2 ⊕ T2;
8. N7 = N3 ⊕ T3;
9. N8 = N4 ⊕ T4;
10. for (i = 9, j = 5; i<=12, j<= 8; i++, j++)
{
Ni = Nj - 0100;
}
11. Extract four 4-bit numbers from LSB position of UID i.e. T5 to T8
12. N13 = N9 ⊕ T5;
13. N14 = N10 ⊕ T6;
14. N15 = N11 ⊕ T7;
15. N16 = N12 ⊕ T8;
16. Decimal numbers of N1 to N16
17. Extract first N0th bit and placed in LSB position of K1
18. for (i=1; i<=15; i++)
{
tempi = Ni-1 + R1; //2's complement of R1
if (Ni+1 ≠ NULL)
{
find the next empty position from LSB;
place tempi bit of K1;
}
else
place tempi bit on Ni+1 th position of K1;
Repeat steps 4 to 19 of S1 algorithm for R2 computation.

2. Encrypting Sender Node UID:

Algorithm S2: -
Input: Sender node UID = 32-bit, two 16-bit keys K1 and K2
Output: encrypted 16-bit UID 'E'.
1. Extract two 16-bit numbers from MSB position of UID i.e. UMSB and ULSB
2. E1 = UMSB ⊕ K1;
3. E2 = ULSB ⊕ K2;
4. E = E1 ⊕ E2;
E is the encrypted 16-bit UID of the sender node.

3. Embedding of Keys:

Algorithm S3: -
Input: Two 4-bit random numbers R1, R2 and encrypted 16-bit UID 'E', sender & receiver node location coordinates (XS, YS), (XR, YR).
Output: 24-bit encrypted UID.
1. Calculate the distance
d = XS + YS + (base3) XR + (Base5) YR;
t2 = binary compliment of d;
dis = decimal value of t2;
2. Insert the R1 and R2 keys in 16-bit encrypted UID
Insert R1 at position dis+1 in 16-bit encrypted UID;
Insert R2 at next position dis+4 in 16-bit encrypted UID;
3. 24 bit encrypted UID

At last we get encrypted 24-bit UID of the sender node which is transmitted for the authentication process at the receiver node side.

Receiver Side Algorithm – The receiver side algorithm also applies the same process as of the sender side algorithm. The receiver node has information related to the location of the sender node and its own. The receiver side algorithm consists of four steps: Keys extraction, Keys Formation, Encrypting Sender Node UID and Check for authentication.

Algorithm R: -
Input: Encrypted 24 bit UID, sender and receiver node location coordinates (XS, YS), (XR, YR)
Output: True or False.

```
1. Receive 24 bit encrypted UID send by the sender node.
2. Calculate the distance
d = XS + YS + (base3) XR + (Base5) YR ;
t2 = binary compliment of d;
dis = decimal value of t2;
3. Extract two 4-bit random numbers R1 and R2 from 24 bit encrypted UID.
if (dis<=8)
{       while (i<=4)
        dis + i    gives R1;
        2*(dis + 4) + i    gives R2;
}
else
{       while (i<=4)
        dis + 4 + i    gives R1;
        2*(dis+4) + i    gives R2;
}
4. Calculate encrypted 16-bit UID i.e. E'.
5. if (E' == E)
{
        Authentication successful;
}
else
{
        Node is cloned;
}
```

From the receiver side algorithm we generate the encrypted 16-bit UID i.e. E'. Now for authentication process both UIDs E (16-bit UID of sender node) and E' (16-bit UID of receiver node) are matched with each other. If both UIDs match absolutely, then node successfully completed the authentication process else the node is designated as clone node. When clone node is identified, a message is broadcasted in the sensor network and clone node is discarded from the WSNs by the base station.

4.4 Performance Analysis of Proposed Node Authentication Algorithm

The proposed algorithm performance is measured by the various mathematical metrics. These metrics are selected on the as per WSNs constraints. Also the proposed algorithm is compared with a number of algorithms from the literature on the basis of the metrics: Clone Detection Probability, Communication Overhead, Computational Overhead, Storage Overhead and Security Level.

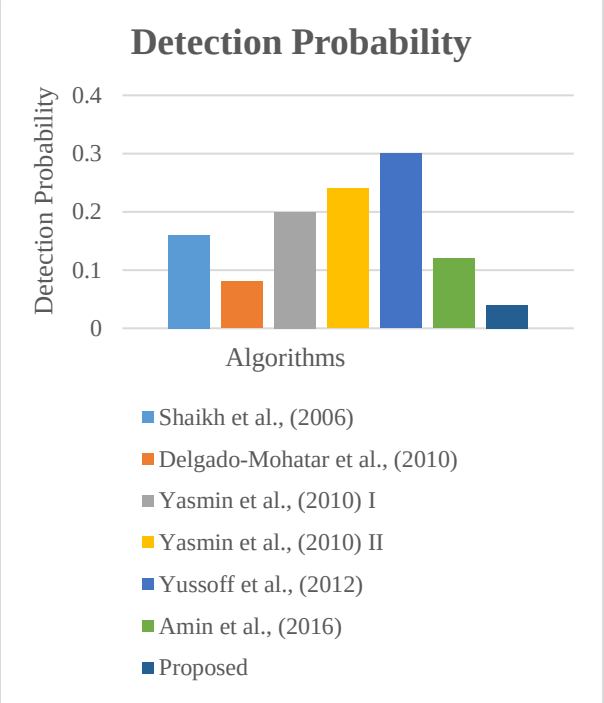


Figure 4.1Clone Detection Probability

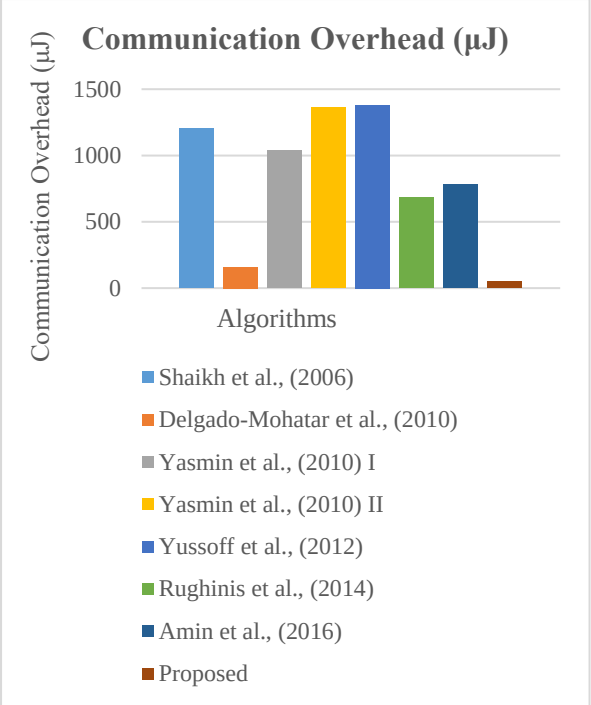


Figure 4.2Communication Overhead

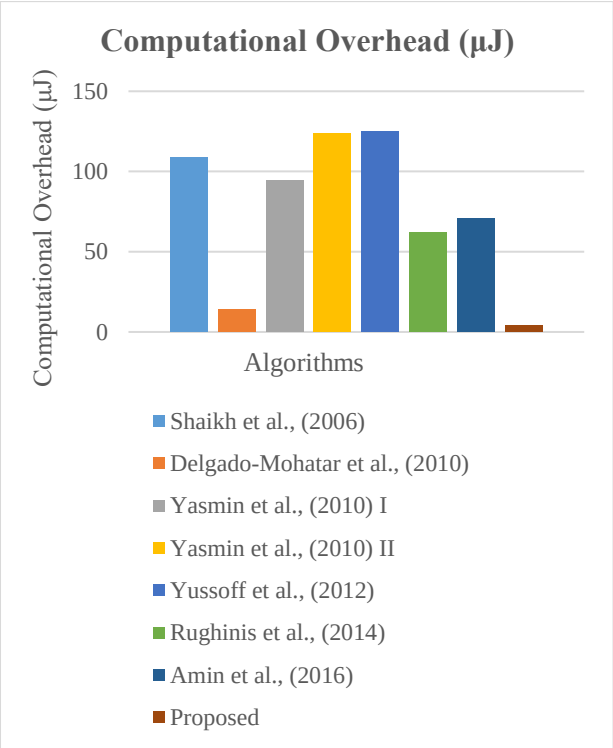


Figure 4.3Computational Overhead

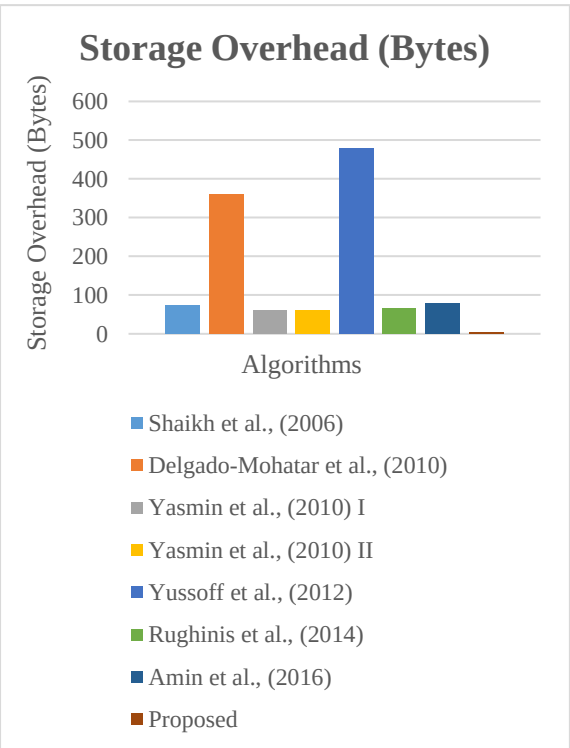


Figure 4.4Storage Overhead

4.4.1 Clone Detection Probability: This is the utmost vital metric used for examining the competence of algorithm [17]. The clone detection probability can be defined as the possibility of successful detection of cloned nodes inside WSNs. The equation for clone detection probability is given by:

$$P = \frac{Total\ number\ of\ successful\ authentication\ with\ clone\ nodes}{Total\ number\ of\ executions} * 100$$

Where P = Clone detection probability

The proposed algorithm has high clone detection probability because of low successful authentication with clone nodes as contrasted with the algorithms shown in figure 4.1. Whenever, clone node tries to communicate with sensor nodes, node authentication process gets initialized automatically, keeping in mind to get the trustworthy node for communication.

4.4.2 Communication Overhead: This is the most significant metric for examining the working of WSNs algorithms. Communication overhead is described as the energy spent during communicating one byte of data.

$E_C = E_T * L$
$E_C = 16.25 * 3$
$E_C = 48.75\ \mu J$

Where, E_T = Transmitting Energy, L = Transmitted Message in bytes
E_C = Communication Overhead

Therefore, from the above calculations and figures of communication overhead, the proposed algorithm add minimum communication overhead (48.75 μJ) to WSNs, which is very a smaller amount when compared with other algorithms as presented in Figure 4.2.

4.4.3 Computational Overhead: Each algorithm required some energy for execution of different computational operations for accomplishing their preferred objective. For the proposed algorithm, computational overhead is the measure of the energy required during the key generation process, the encryption process and embedding process.

$E_{CP} = E * Clock\ Cycles$
$E_{CP} = 0.0032 * 1380$
$E_{CP} = 4.416\ \mu J$

Where, E = Energy required per clock cycle
E_{CP} = Computational Overhead

The proposed algorithm requires 1380 clock cycles for completing its execution and results in 4.416 μJ of computational overhead. Figure 4.3 gives the computational overhead of various node authentication algorithms.

4.4.4 Storage Overhead: Storage overhead can be defined as the measure of information saved in the memory of sensor nodes during algorithm execution. In the proposed calculation sensor nodes store 3 bytes of information during algorithm functioning which is depicted in figure 4.4.

4.4.4 Security Level: The proposed algorithm utilized static location coordinated of sender and receiver nodes that remain fixed during the WSN working. Thus, the proposed node authentication algorithm gives a high security against node clone attack.

However, even after implementing this proposed node authentication algorithm if some cloned node left undetected within wireless sensor networks, then the message authentication algorithm is implemented before actual message communication starts. The next chapter solves this problem by proposing a new message authentication technique.

CHAPTER 5
MESSAGE AUTHENTICATION: NODE CLONE ATTACK

5.1 Introduction

Wireless Sensor Networks (WSNs) [1], [18] are autonomous systems which primarily work with data gathered from the physical environment. The basic building block of WSN is sensor nodes [19],[20].The main challenge for securing energy-constrained networks from various attacks is that the mechanism must be lightweight and robust. Traditional cryptographic algorithms do not work well with the WSNs because asymmetric encryption and digital signature are too costly and computationally impractical. Further, symmetric encryption algorithms have to be used economically so that sensor node remains alive during the network lifetime [21].This chapter proposed a novel method for securing message communication in resource-constrained WSNs. This method is highly efficient in terms of security i.e. authenticity & integrity of messages remains while communication. And also, energy overheads are minimized.

5.2 Proposed Message Authentication Algorithm

The aim of the proposed message authentication algorithm is to authenticate messages that are being communicated within the open unsafe sensor networks. The proposed message authentication algorithm easily identifies the messages coming from clone node and it saves sensor node energy. The proposed message authentication algorithm consists of two parts: Hash Calculation Algorithm and Message Authentication Algorithm.

Hash Calculation Algorithm: In the hash calculation algorithm, the fixed hash digest is calculated from the message of arbitrary length. The hash digest is robust enough to secure message communication.

Algorithm Hash_Compute (msg)
Input: Message string X of arbitrary length.
Output: Hash digest (H) of 24 bits.
1. Convert input message into ASCII numbers of the respective characters.
2. Now convert each character into an 8 bit binary number.
3. Apply unambiguous padding in the LSB to make divisible by 512.
4. Generate a 96 bit array ‘A1’ of prime numbers (first 96 prime).
5. Now the preprocessed message is split into:
Each 512 bit block is divided into 8, 64 bit blocks.
Each 64 bit block is divided into 8, 8 bit blocks.
6. Firstly, substitution of each 8 bit block takes place by a prime number selected by the A1 table.
7. The values for each 8, 8 bit blocks generated.
8. XOR operation on 8, 8 bit block is applied and results in values for each 8, 64 bit blocks.
9. Now values for 67 bit array ‘A2’ table are calculated. The A2 table takes prime number above 2048 (12 bit values).
10. Apply Mod 67 operation to above calculated 8, 8 bit values (to get values in range 0-66).
11. The second substitution of each 8, 64 bit block takes place with A2 table values.
12. We receive 96 bit values i.e. H1 to Hn for every 512 bit block.

13. Binary Addition applied on each 512 bit values

H = H1 + H2 + H3 +……..+ Hn.

14. At last, hexadecimal conversion is applied on H to get 24 bit values.
15. A hash digest (H) of 24 bit generated.

The calculated 24 bit hash digest is vigorous enough that changes in one-bit position in the message result in the different hash digest.

Message Authentication Algorithm: Message authentication algorithm used to authenticate the message received by the sensor node. If message during communication captured or modified by the cloned node, it can easily authenticate. Minor change in message changes the calculated hash digest.

Algorithm M
Input: Message and hash digest (H)
Output: Message Authentication
1. Let ith sender node wants to communicate with the jth sensor node. It sends a message along with its 24-bit hash digest (H) to the receiver node.
2. At the receiver end, jth sensor node receives the message and 24-bit hash digest (H).
3. Receiver node again computes the new hash digest (H') from the received message.
4. The values of H with H' are compared at the receiver node.
5. if (H' = = H)
{
Message is authenticated
}
else
{
Message modified by Cloned node
}

In the last step, both calculated hash digests i.e. H and H' are compared to check the authenticity of the message that is communicated by the sender node. If both H and H' are same then the message is sent by authentic sender node otherwise message is send by cloned sensor node. A slight change in the message will result in the different hash digest.

5.3 Results and Analysis of Proposed Message Authentication Algorithm

This section discusses the results and analysis of the proposed message authentication algorithm. Analysis of the proposed algorithm is done by following performance metrics: Clone Detection Probability, Communication Overhead, Computational Overhead, Storage overhead and Security level.

5.3.1 Clone Detection Probability: Clone detection probability is the best metric in order to identify cloned nodes and calculate the efficiency of the proposed message authentication algorithm. Clone detection probability is the total number of successful message authentication with clone nodes divided by the total number of algorithm executions [22]. The formula for Clone detection probability is given below:

$$P = \frac{(\text{Total number of successful message authentication with clone nodes})}{(\text{Total number of executions})} * 100$$

Where, P is the Clone detection probability

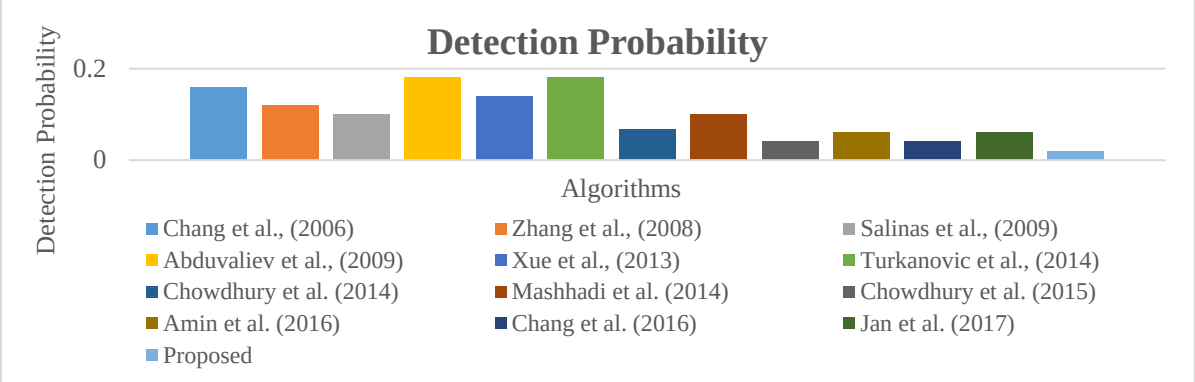


Figure 5.1Clone Detection Probability

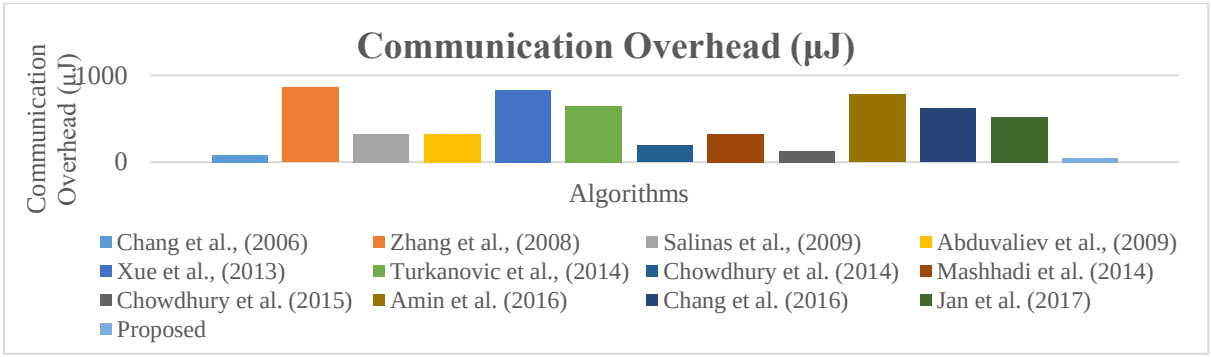


Figure 5.2Communication Overhead

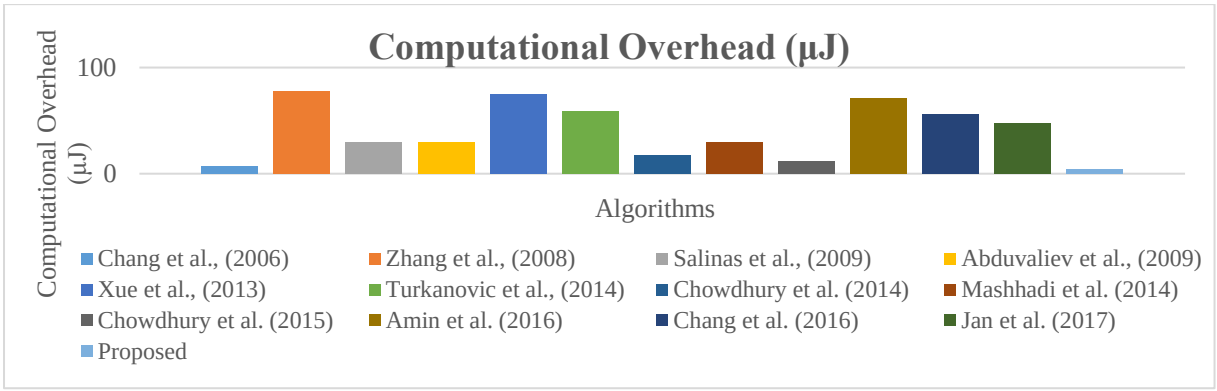


Figure 5.3 Computational Overhead

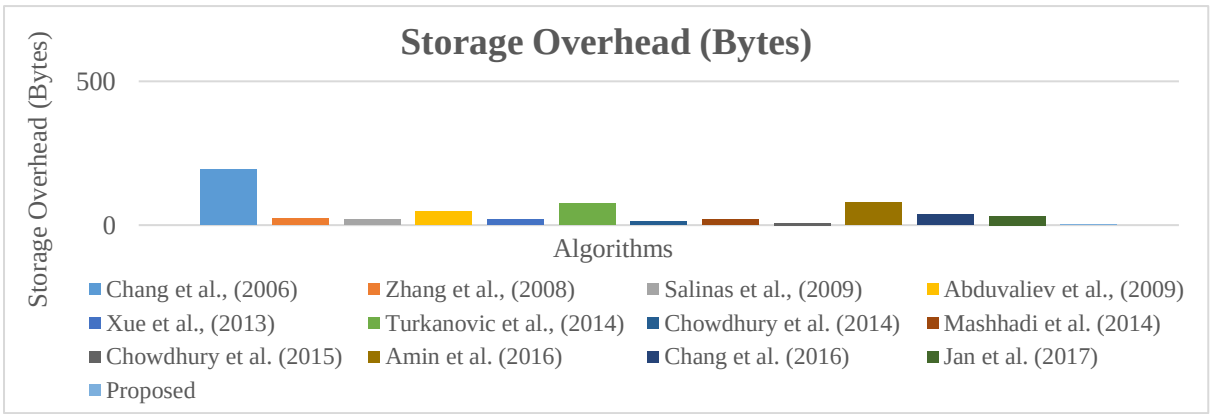


Figure 5.3 Storage Overhead

Figure 5.1 represents the clone detection probability of message authentication algorithms. The proposed algorithm uses one-way 24-bit fixed hash digest to check the authenticity and integrity of messages.

5.3.2 Communication Overhead: Communication overhead is defined as the sum of energy disbursed for communicating one (1) byte of data in WSNs.

$$E_C = E_T * L$$
$$E_C = 16.25 * 3$$
$$E_C = 48.75\ \mu J$$

Where, E_T = Transmitting Energy
L = Transmitted Message in bytes
E_C = Communication Overhead

Figure 5.2 represents the communication overhead of message authentication algorithms in WSNs. The proposed message authentication having 48.75 μJ communications overhead which is not as much of as related to other existing algorithms.

5.3.3 Computational Overhead: This overhead is defined by the quantity of energy required during message authentication process. As the proposed message authentication algorithm include mod, XOR, split and transformation operations that require very less amount of sensor node energy.

$$E_{CP} = E * \text{Clock Cycles}$$
$$E_{CP} = 0.0032 * 1380$$
$$E_{CP} = 4.416\ \mu J$$

Where, E = Energy required per clock cycle
E_{CP} = Computational Overhead

Figure 5.3 gives the pictorial presentation of the computational overhead comparison of various algorithms with the proposed algorithm in sensor networks.

5.3.4 Storage Overhead: Storage overhead can be defined as the quantity of data stored in the sensor node memory [23]. The proposed message authentication algorithm stores 3 bytes of data in the sensor node memory. For this, we only check the extra storage space needed by each algorithm in order to store the data during the message authentication process. Figure 5.4 represents the comparison of various existing algorithms and proposed algorithm in relation to storage overhead in WSNs.

5.3.5 Security level: Foremost prerequisite of any wireless sensor networks algorithm is the high level of security. The security in these sensor networks is violated by various active as well as passive attacks. Therefore, proposed message authentication algorithm focus on authenticity and integrity of messages during communication in WSNs.

This proposed algorithm is fit to the energy inhibited WSNs because proposed algorithm is light-weight in terms of communication, computation and storage overhead with respect to all other algorithms. Further, the proposed algorithm gives low successful message authentication with clone sensor nodes, therefore, on the other side results in higher Clone detection probability as compared to the existing algorithms.

CHAPTER 6

MOBILE NODE AUTHENTICATION IN WIRELESS SENSOR NETWORKS

6.1 Introduction

Mobile Wireless Sensor Networks (MWSNs) consists of spatially distributed static sensor nodes [24], [25] and a fraction of mobile sensor nodes in the Region-of-Interest (RoI). The fraction of mobile nodes is advantageous over a complete static wireless sensor network in terms of several Quality-of-Service parameters such as energy efficiency, coverage, connectivity etc. [26]. Further, security [27] is an important issue in MWSN due to the dynamic nature of the mobile nodes [28], [29]. Node mobility is the main concern in several application scenarios such as the Intelligent Transportation System and healthcare scenario.

Therefore, our motivation is to present an energy-efficient, low overhead re-authentication scheme approach [30], [31]. Re-authentication is important for a mobile node as the node moves from one region to another region in the RoI. In this chapter, we present the Re-authentication approach for mobile nodes in the network. In this work, we design an authentication framework for securing MWSN [32]. The proposed protocol is compared with existing mobile node authentication protocols available in the literature [33], [34].

6.2 The Proposed Protocol for Mobile Node Re-Authentication

The sensor nodes are organized into Voronoi based cluster architecture. The members of the Voronoi based clusters are static nodes or mobile nodes. The cluster head is responsible for management activities in its Voronoi regions. The activities include coordination with members, coordination with neighbor Voronoi CH, and sending data to the Base Station. Hierarchical architecture helps to achieve better scalability compared to a flat architecture where all the nodes are peers. The proposed algorithm include following steps:

6.2.1 Mobile Node Management

For an effective mobile-node management each CH maintains two tables. The first table is known as the home table and the second is the visitor table. Home table maintains the list of all the mobile nodes which are assigned to a Voronoi region. Visitor table keeps track of the entire mobile nodes visitor to a particular Voronoi region. Inter-cluster communication among CH performs effective management of the mobile nodes. The following steps are typical for a mobile node:

- Mobile node moves on-demand basis to the different Voronoi region and connects itself to the CH. CH then updates the visitor table whereas previous CH of a mobile node updates its home table.
- Whenever the foreign mobile node leaves the Voronoi region the CH deregisters the node entry from its foreign table.

6.2.2 Network Setup phase

The network divides the Region-of-Interest into Voronoi cells where each Voronoi head is designated as the Voronoi region cluster head. Let Vi and Vj be the cluster heads for ith and jth Voronoi regions respectively. The Voronoi cluster heads are deployed based on well-known deployment techniques available in the literature. Further, the neighbor list for ith Voronoi cluster head Vi is given by NGH(Vi). During the network setup phase base station distributes a set of IDs to each of the Voronoi Region cluster heads (CHs) using a secure channel.

6.2.3 Registration phase of the mobile node

The mobile node first registers at the home cluster head of the corresponding Voronoi region say Vi. The mobile node obtains its identification (Mm), the hash value H(Mm), a random number (Ri), shared a secret key (xmi) and a pairwise session key (KViMm) from Vi via offline distribution in a secure manner.

(1) Initialization: The mobile node sends its identification Mm along with the hash value H(Mm) to home cluster Vi. The mobile node Mm starts the process of joining the network by sending the following message to Vi: Exmi {Vi|| Mm || KViMm }.

(2)On receipt of the message from Mm, Vi computes DxmiExmi{ Vi|| Mm || KVi Mm }. The entries for the mobile node Mm is searched for the pre-register identifier in Vi. If the match is found the step (3) executes else exit.

(3)The Voronoi node Vi sends Exmi{ Vi|| Mm || KVi Mm ||R1 } to Mm.

(4)Mm receives the message and recovers the following values: Vi|| Mm || KVi Mm ||R1.

The mobile nodes have the information Mm , H(Mm), pairwise session key KVi Mm , a random number R1, Ri after being authenticated from home cluster Vi.

6.2.4 Mobile Re-authentication phase

The mobile node can now reside in its home cluster Vi or move to foreign cluster Vj in the network. Further, Vj can be an immediate neighbor or τ hop neighbor of Vi. In case, Vj is τ hops neighbor of Vi, Vj is reachable from Vi . We observe that based on the movement of the mobile node (Mm) three conditions are possible:

Case 1: Mm lies in the same Voronoi region. The mobile node communicates with the network using the authentication code: MAC(KViMm,m).

Case 2: Mm lies in the different Voronoi region Vj. Vj is τ hops ($0<\tau<$ network diameter) from Vi in a connected network.

Case 3: Mm lies in the different Voronoi region Vj. Vj is not connected from Vi. This case arises in due to a break in the connectivity of the network. Since Mm is mobile it moves to adjoining Voronoi region for re-authentication and communication with the network.

Case 1 is the authentication in the same home cluster as stated in the registration phase of the mobile node. We now explain Case 2 in detail where Vj is τ hops ($0 < \tau <$ network diameter) from Vi in a connected network. On visiting a foreign region Vj the mobile node (Mm) tries to re-authenticate with the cluster Vj. The re-authentication phase is carried out whenever a mobile node visits a foreign network and wants to gain access to the network via foreign cluster head Vj.

6.2.5 Mobile Re-authentication phase

The mobile node moves into Voronoi region Vj and sends the re-authentication request to Vj node. The hello message is passed to Vj along with (Mm || Vi)values. Upon receipt of the message the routing path is searched in Vj. If routing path is not found in Vj then route setup for on-demand basis is made from Vj to Vi node. Upon successful route setup reply message is passed to mobile node in single hop. Further, the route setup process is followed by the re-authentication phase by Vj node.

6.2.6 Re-authentication phase

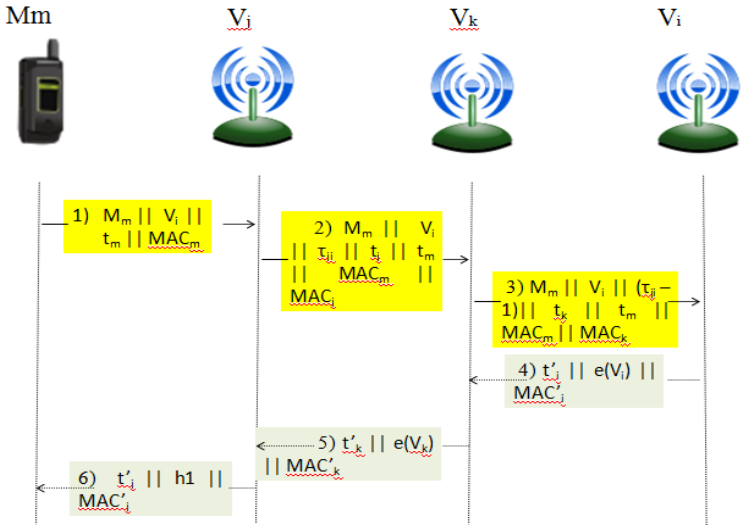


Figure 6.7: Our proposed scheme for re-authentication process for Mobile node Mm with the help of 3 clusterhead(Vj ->Vk -> Vi) and back (Vi ->Vk->Vj)

6.3 Performance Analysis

In this section we present the performance analysis of our proposed protocol. We present the communication passes, message size, energy consumption, and computation cost involved in the re-authentication process.

6.3.1 Communication Pass: Figure 6.4 presents the number of communication passes versus a number of Voronoi regions for non-neighbor Voronoi regions. Our scheme works for adjacent neighbor as well as non-adjacent neighbor roaming scenario. Prior to re-authentication phase on-demand route setup phase establishes the routing path among foreign and home cluster heads. This leads to the better scalability of the network in a dynamic scenario. Further, on-demand route setup for mobile nodes re-authentication is better as compared to pre-computed information during setup with the help of base station for better scalability of the network. However, our scheme leads to overhead for On-demand route setup phase.

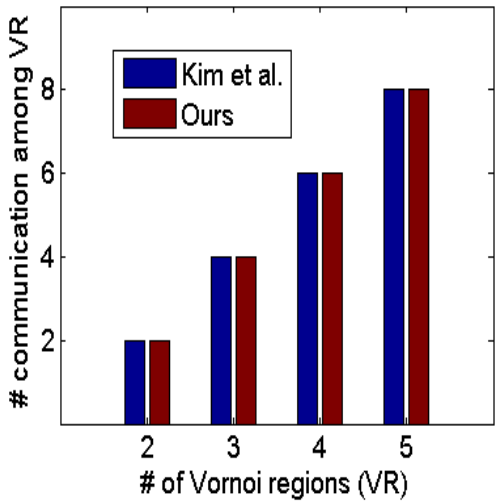


Figure 6.1Communication Pass

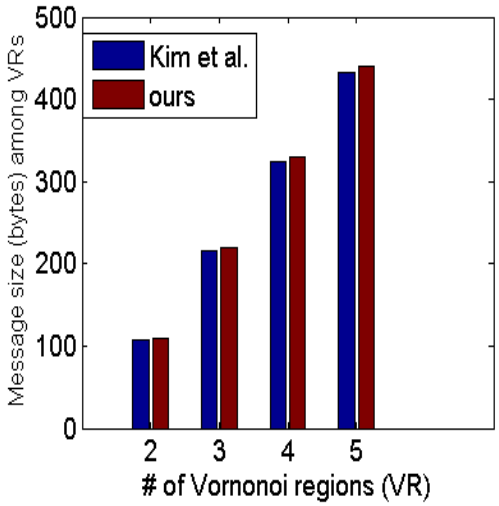


Figure 6.2Message Size

6.3.2 Message Size: Several researchers we use the message settings size as follows: MAC size is 4 bytes, timestamp is 8 bytes, a random number is 8 bytes, identification is 1 byte and key size is 16 bytes [195]. Further, in our work we introduce an additional 1 byte for a number of hops from source to destination cluster heads. Figure 6.5 presents the message size in bytes versus a number of Voronoi regions for non-neighbor Voronoi regions.

6.3.3 Energy Consumption: Similar to the parameters of Kim et. al., (2017) [35] we compute transmission and reception energy as 16.25 μJ/byte and 12.5 μJ/byte respectively. We compare only the non-neighbor case in the re-authentication case. We observe that energy consumption for non-neighbor case (Kim et. al., 2017) [35] is comparable with our proposed scheme (Refer Figure 6.3).

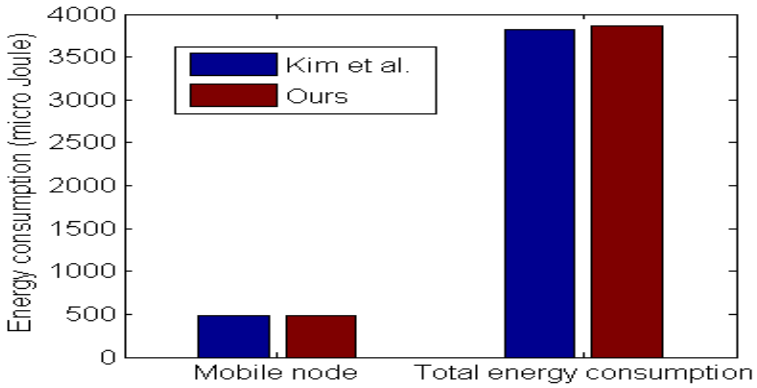


Figure 6.3Energy Consumption

6.3.4 Computation Cost: Re-authentication scheme consumes 2 Encryption/Decryption in node. Re-authentication scheme consumes 4Encryption/Decryption in total.

Table 6.1Computation Cost

	Jiang et. al., 2011 [36]	Kim et. al., 2017 [35]	Our Proposed
Total number of Encryption / Decryption	4	4	4
Encryption/Decryption in node	2	2	2
Total number of MAC generation/verification	4	4	4
MAC generation/verification in node	2	2	2

In this work, we propose an authentication framework for securing mobile nodes in WSN. The proposed framework ensures mobile node authentication for different cases. The first case is when a mobile node travels to an adjacent cluster region. The second case refers to when the mobile node moves to a non-neighbor cluster region which may be several hops away from the initial position of a mobile node. Further, performance analyses for our re-authentication scheme and provides the comparison with the other re-authentication scheme present in the literature. The analyses results show that our scheme has a comparable performance on communication overhead, message size, and computation cost compared with the schemes present in the literature. Further, the proposed scheme provides scalable architecture for MWSN.

CHAPTER 7

CONCLUSION AND FUTURE SCOPE OF WORK

7.1 Introduction

In wireless sensor networks, sensor nodes carry information from one part of the network to another part of the network. Due to the nature of sensor nodes deployment and resource-constrained limitation WSNs becomes susceptible to a wide variety of attacks. As wireless sensor network consists of static as well as mobile nodes vulnerable to attacks, it is important to secure these sensor nodes from the adversary. Authentication is the one of the critical security requirement which secures WSNs from the security attacks.

In this thesis, we contributed to overcoming these challenge in wireless sensor networks. Firstly, hybrid cryptography algorithm is proposed in Chapter 3 which secures sensor networks from the critical node clone attack. This algorithm comprises of AES and ECC cryptography algorithm that helps in securing messages communication within the sensor networks. Further, the hash function used in this work maintains the integrity of the message. From the proposed algorithm it can be concluded that the algorithm overcomes the security problem and provides authentication and confidentiality in the WSNs. The proposed algorithm lowers the computational and communication overheads. However, it increases storage overhead in the network.

In our next work in Chapter 4, we present the node authentication algorithm for securing sensor nodes. The sensor nodes in WSNs are susceptible to node clone attack where attacker negotiates the node and pull out confidential information from sensor node and further reproduce the numbers of clones and spread the clone nodes within the sensor network. The proposed algorithm, authenticate the sensor nodes in the initial step of the message communication. This algorithm is designed to be energy efficient as it uses simple encryption, decryption operations and extraction, bitwise shift, and XOR, operations. From this proposed algorithm is can be concluded that, the sensor nodes are checked for their originality and clone or fake nodes are easily identified by the proposed algorithm. This algorithm checks the sensor nodes at the very initial stage of communication. The performance of the proposed algorithm is a good option for any energy-constrained networks. The algorithm minimizes the energy utilization in the wireless sensor network. The algorithm has high clone detection probability rate.

However, after securing the sensor nodes, messages moving within sensor networks need to secure from the node clone attack. Clone node eavesdrop messages while communication between genuine nodes in WSNs. After snooping they can modify the messages and then generate a reply attack. Therefore, it is important to secure message communication from the security attacks. To solve this problem we proposed the new lightweight message authentication algorithm for securing message communication in WSNs. The objective of the algorithm is to ensure message authentication and integrity. The algorithm uses *Mod* and *XOR* operations to compute fixed size hash value or message digest. From this work, we conclude that, the algorithm is robust as a minor variation in the message will change the entire hash value. Also, this message authentication algorithm is effortlessly implemented on energy-constrained networks and provides secure message communication and integrity in WSNs.

Mobile Wireless Sensor Networks (MWSNs) is advantageous over a complete static wireless sensor networks in terms of Quality of Service parameters. Mobile sensor nodes are very dynamic in nature; their position keeps on changing from time to time. Therefore, it is very difficult to find out the exact location of mobile nodes. For WSNs, the mobility of sensor

nodes brings security issue like re-authentication and locating the sensor node movement. In this work, we propose an authentication framework for securing mobile nodes in WSNs. A fraction of the nodes are mobile and the rest of the nodes are static nodes. The proposed framework ensures mobile node authentication for two different cases. The first case is when a mobile node travels to an adjacent Voronoi cluster region. The second case refers to when the mobile node moves to a non-neighbor Voronoi cluster region which may be several hops away from the initial position of a mobile node. In this work, we propose a re-authentication scheme for mobile wireless sensor networks. The re-authentication scheme ensures security in mobile wireless sensor networks and provides prevention against node compromise attacks. From this contribution of work it is concluded that, mobile nodes are easily secured by the re-authentication process.

From the above discussion it is clear that, all four algorithms proposed in this thesis is the best suitable for WSNs applications. The algorithms are designed in an energy efficient manner keeping in mind the energy constraints sensor nodes. Further, these proposed algorithms secure WSNs from various critical attacks like node clone attack, Sybil attack, wormhole attack, denial of service attack, etc. These algorithms enhance the efficiency of the network and network lifetime.

7.2 Limitations of Work

We perceive the following limitations of our proposed work:

1. In Chapter 3, the hybrid cryptography algorithm uses cryptographic encryption and decryption algorithms that provide a high level of security but these algorithms use an excess of sensor node energy. This proposed algorithm is not a good option for implementing on energy-constrained networks.

2. The proposed node authentication algorithm in Chapter 4, authenticate or validate the static sensor nodes in WSNs. This algorithm does not work on mobile sensor nodes.

3. In Chapter 5, message authentication algorithm can only work on static wireless sensor networks where sensor node position remains fixed during the whole network lifetime.

7.3 Future Work

Wireless Sensor Networks gain more and more attention day by day, therefore there is need focus on various challenges to face by this ever-growing technology. In this we took one of the issues of WSNs i.e. Security. As these sensor networks are open to all and anyone can look up or interfere in the normal functioning. Securing sensor nodes and message communication in WSNs is one of the most precarious tasks. In this thesis we presented four algorithms for securing sensor nodes as well as message communication in WSNs.

Hybrid cryptography algorithm uses highly constrained encryption and decryption cryptography algorithms. The algorithm can be optimized in the future by designing encryption and decryption algorithm that utilizes very low computation and memory cost. Further, node authentication algorithm only designed for static sensor node and the location of static sensor node is one of the parameters in the algorithm. In the future, we can extend this algorithm for mobile sensor nodes for authentication. Similarly, in the case of message authentication algorithm we only tested algorithm for static sensor nodes. In the future, we can extend our research towards mobile sensor nodes so that much real-world application can get benefited with our proposed algorithm. In addition, a re-authentication mechanism which is proposed for mobile sensor nodes in wireless sensor networks can be tested for a number of dynamic applications like military application, healthcare monitoring, Body sensor networks, traffic monitoring, forest fire detection, wildlife monitoring, etc.

References

[1] Yick, J., Mukherjee, B. and Ghosal, D., *"Wireless sensor network survey"*, Computer networks, vol. 52, no. 12, pp. 2292-2330, 2008.

[2] Wang, Y., Attebury, G. and Ramamurthy, B., "*A survey of security issues in wireless sensor networks",* IEEE Communications Surveys & Tutorials, vol. 8, no. 2, pp. 2-23, 2006.

[3] Walters, J.P., Liang, Z., Shi, W., and Chaudhary, V., *"Wireless sensor network security: A survey"*, Security in distributed, grid, mobile, and pervasive computing, vol. 1, pp. 367 2007, 2007.

[4] Jan, M., Nanda, P., Usman, M. and He, X., *"PAWN: a payload-based mutual authentication scheme for wireless sensor networks"*, Concurrency and Computation: Practice and Experience, vol. 29, no. 17, pp. 3986, 2017.

[5] Kumari, S., Khan, M.K. and Atiquzzaman, M., *"User authentication schemes for wireless sensor networks: A review"*, Ad Hoc Networks, vol. 27, pp.159-194, 2015.

[6] Hayouni H, Hamdi M, Kim T-H, *"A Survey on Encryption Schemes in Wireless Sensor Networks",* Proc. of the 7th International Conference on Advanced Software Engineering and Its Applications (ASEA), China, pp. 39-43, 2014.

[7] Si L, Ji Z, Wang Z., *"RETRACTED: The Application of Symmetric Key Cryptographic Algorithms in Wireless Sensor Networks"*, Physics Procedia of International Conference on Solid State Devices and Materials Science, Macao, vol. 25, pp. 552-559,2012.

[8] Dargie, W. and Poellabauer, C., *"Fundamentals of wireless sensor networks: theory and practice"*, John Wiley & Sons, 2010.

[9] Romer, K., Kasten, O., and Mattern, F., *"Middleware challenges for wireless sensor networks"*, ACM SIGMOBILE Mobile Computing and Communications Review, vol. 6, no. 4, pp. 59-61, 2002.

[10] Conti, M., Pietro, R.D., Mancini, L.V., and Mei, A., *"Distributed detection of clone attacks in wireless sensor networks"*, IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 5, pp. 685-698, 2011.

[11] D. Sheela and G. Mahadevan, *"Efficient approach to detect clone attacks in Wireless sensor Networks"*, Proc. IEEE 3rd International Conference on Electronics Computer Technology (ICECT), pp. 194-198, 2011.

[12] Zheng, Z., Liu, A., Cai, L.X., Chen, Z., and Shen, X., *"ERCD: An energy-efficient clone detection protocol in WSNs"*, Proc. IEEE INFOCOM, pp. 2436-2444, 2013.

[13] Rizk R, Alkady Y., *"Two-phase hybrid cryptography algorithm for wireless sensor networks"*, Journal of Electrical Systems and Information Technology, vol. 2, no. 3, pp. 296-313, 2015.

[14] Amin NU, Asad M, Chaudhry SA., *"An authenticated key agreement with rekeying for secured body sensor networks based on hybrid cryptosystem"*, Proc. of the 9th IEEE

International Conference on Networking, Sensing and Control (ICNSC), Beijing, pp. 118-121,2012.

[15] Anita EAM, Geetha R, Kannan E., *"A novel hybrid key management scheme for establishing secure communication in wireless sensor networks",*Journal of Wireless Personal Communications, vol. 82, no. 3, pp. 1419-1433,2015.

[16] Lu H, Li J, Guizani M., "*Secure and efficient data transmission for cluster-based wireless sensor networks"*, IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 3, pp. 750-761,2014.

[17] Romer, K., Kasten, O., and Mattern, F., *"Middleware challenges for wireless sensor networks"*, ACM SIGMOBILE Mobile Computing and Communications Review, vol. 6, no. 4, pp. 59-61, 2002.

[18] Borges, L.M., Velez, F.J. and Lebres, A.S., *"Survey on the characterization and classification of wireless sensor network applications"*, IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp.1860-1890, 2014.

[19] Rault, T., Bouabdallah, A. and Challal, Y., *"Energy efficiency in wireless sensor networks: A top-down survey"*, Computer Networks, vol. 67, pp.104-122,2014.

[20] Rawat, P., Singh, K.D., Chaouchi, H., and Bonnin, J.M., *"Wireless sensor networks: a survey on recent developments and potential synergies"*, The Journal of supercomputing, vo. 68, no. 1, pp. 1-48, 2014.

[21] Shim, K.A., "*A survey of public-key cryptographic primitives in wireless sensor networks"*, IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp.577-601, 2016.

[22] Aalsalem, M.Y., Khan, W.Z., Saad, N.M., Hossain, M.S., Atiquzzaman, M., and Khan, M.K., "*A New Random Walk for Replica Detection in WSNs*", PloS one, vol. 11, no. 7, pp. e0158072, 2016.

[23] Ghosal, A., Halder, S. and DasBit, S., *"A dynamic TDMA based scheme for securing query processing in WSN".* Wireless Networks, vol. 18, no. 2, pp.165-184, 2012.

[24] Mohindru, V. and Singh, Y., *"Node authentication algorithm for securing static wireless sensor networks from node clone attack*", International Journal of Information and Computer Security, vol. 10, no. 2-3, pp.129-148,2018.

[25] Khoufi, I., Minet, P., Laouiti, A. and Mahfoudh, S., "*Survey of deployment algorithms in wireless sensor networks: coverage and connectivity issues and challenges",* International Journal of Autonomous and Adaptive Communications Systems (IJAACS), vol. 10, no. 4, pp. 341-390, 2017.

[26] Yetgin, H., Cheung, K.T.K., El-Hajjar, M. and Hanzo, L.H., "*A survey of network lifetime maximization techniques in wireless sensor networks",* IEEE Communications Surveys & Tutorials, vol. 19, no. 2, pp.828-854,2017.

[27] Radhappa, H., Pan, L., Xi Zheng, J. and Wen, S., *"Practical overview of security issues in wireless sensor network applications",* International Journal of Computers and Applications, pp.1-12,2017.

[28] Kobo, H.I., Abu-Mahfouz, A.M. and Hancke, G.P., "*A Survey on Software-Defined Wireless Sensor Networks: Challenges and Design Requirements",* IEEE Access, vol. 5, no. 1, pp.1872-1899,2017.

[29] Rani, A. and Kumar, S., "*A survey of security in wireless sensor networks*", 3rd International Conference on Computational Intelligence & Communication Technology (CICT), IEEE, pp. 1-5, Feb. 2017.

[30] Xie, Q.Q., Jiang, S., Wang, L. and Chang, C.C., "*Composable Secure Roaming Authentication Protocol for Cloud-assisted Body Sensor Networks*", IJ Network Security, vol. 18, no. 5, pp.816-831,2016.

[31] Banerjee, P., Chatterjee, T. and DasBit, S., "*LoENA: Low-overhead encryption based node authentication in WSN*",IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 2126-2132, Aug. 2015.

[32] Sabor, N., Sasaki, S., Abo-Zahhad, M. and Ahmed, S.M., "*A comprehensive survey on hierarchical-based routing protocols for mobile wireless sensor networks: review, taxonomy, and future directions",* Wireless Communications and Mobile Computing, 2017.

[33] Zhiping, Z., Nannan, S. and Xuebo, Z., "*A novel authentication protocol for mobile nodes in multi-base-station wireless sensor network",*019-8, 2014.

[34] Rajeswari, S.R. and Seenivasagam, V., "*Comparative study on various authentication protocols in wireless sensor networks",* The Scientific World Journal, 2016.

[35] Kim, B. and Song, J., "*An efficient and practical mobile node reauthentication scheme for mobile wireless sensor networks",*Proc. of the 3rd International Conference on Communication and Information Processing,ACM, pp. 326-331, Nov.2017.

[36] Jiang, S., Miao, J. and Wang, L., "*Mobile node authentication protocol for crossing cluster in heterogeneous wireless sensor network*", IEEE 3rd International Conference on Communication Software and Networks (ICCSN), pp. 205-209, May 2011.

List of Publications

1. **V. Mohindru**, and Y. Singh, "Efficient Approach for Securing Message Communication in Wireless Sensor Networks from Node Clone Attack," *Indian Journal of Science and Technology*, vol. 9, no. 32, 2016, pp. 1-7. DOI:10.17485/ijst/2016/v9i32/10072.
2. **V. Mohindru,** and Y. Singh, "Node authentication algorithm for securing static wireless sensor networks from node clone attack", *International Journal of Information and Computer Security*, Inderscience Publishers, vol. 10, no. 2-3, 2018, pp. 129-148.DOI: 10.1504/IJICS.2018.091462
3. **V. Mohindru**, R. Bhatt and Y. Singh, "Securing Wireless Sensor Network from Node Clone Attack: A Lightweight Message Authentication Algorithm", *International Journal of Information and Computer Security*, Inderscience Publishers.
4. **V. Mohindru**, and Y. Singh, "Performance Analysis of Message Authentication Algorithms in Wireless Sensor Networks", *In Proc. 4th IEEE International Conference on Signal Processing, Computing and Control (ISPCC- 2017),* Waknaghat, India, 2017, pp. 468-472.DOI: 10.1109/ISPCC.2017.8269724.
5. **V. Mohindru**, and Y. Singh, "Efficient Approach for Securing Message Communication in Wireless Sensor Networks from Node Clone Attack," *In International Conference on Recent Innovations in Computer Science and Information Technology (RICSIT – 2016),* Shimla, India, pp. 1-7.DOI:10.17485/ijst/2016/v9i32/100725.
6. **V. Mohindru**, and Y. Singh, *Wireless Sensor Networks Security Attacks a Node Clone Attack*, Lambert Academic Publishing, ISBN-13: 978-3-659-80624-7, ISBN-10: 3659806242.

Communicated Paper(s)

7. **V. Mohindru**, R. Bhatt and Y. Singh, "Hybrid cryptography algorithm for securing WSNs from node clone attack", *Recent Advances in Electrical & Electronic Engineering.*
8. **V. Mohindru**, R. Bhatt and Y. Singh, "Mobile Node Authentication in Wireless Sensor Networks", *Sustainable Computing: Informatics and Systems (SUSCOM).*
9. **V. Mohindru**, Y. Singh, R. Bhatt and AK. Gupta, "A Review on Security Attacks in Wireless Sensor Networks, *Recent Patents on Engineering.***
10. **V. Mohindru**, R. Bhatt and Y. Singh, "Performance Analysis of Lightweight Node Authentication Algorithms in Wireless Sensor Networks, In Proc. 5th IEEE International Conference on Parallel, Distributed and Grid Computing (PDGC-2018), Waknaghat, India.